بسم الله الرحمن الرحيم

٢٠١١

--- عدة خطوات يمكن أن تفيد في الحماية من تجسس الهاكر عليك --

-

اولاً :

لا تدع المايك (مسجل الصوت)موصول على المقبس المخصص له اثناء عملك على الانترنت إذا لم يكن له حاجة لان الهاكر او المتجسسين إذا اخترقوا كمبيوترك يستطيعون التجسس على الاصوات التي تصدرها من دون علمك .

ثانياً:

كذلك الحال على كاميرا الويب لا تدعها موصولة اذا لم تكن تعمل عليها فيمكن أن يقوم بتشغيله من دون أن تنتبه لان الذي يخترق جهازك يستطيع التحكم بكافة العمليات التي تقوم بها انت وبشكل اسرع منك واسهل لان كافة الادوات تكون جاهزة عنده لكثرة وتعدد هذه البرامج الخبيثة فيستطيع المخترق :

-حذف ملفاتك والتجسس على الكيبورد يعني اي شيء تكتبه يراه .

-ادارة الريجيستري بشكل كامل والحذف والتعديل عليه.

-ايقاف تشغيل الكمبيوتر .

-القدرة على سحب كلمات السر التي تستعمله في الدخول الى حساباتك لذى انصح بحذف ملفات الكوكيز باستمرار(وهي التي يتم فيها حفظ كلمات السر بشكل مشفر ويقوم الهاكر بفك تشفيرها

)فعن طريق الضغط على ctral-shift-delete في الكيبورد لمستخدمي مستعرضات الانترنت الحديثة او الدخول الى -ابدأ>لوحة التحكم >خيارات انترنت > عام >حذف ملفات الاستعراض اوالملفات المؤقتة وملفات تعريف الارتباط (تختلف المسميات حسب اصدارت المستعرض)

يتم التخلص من كل الباسورد المحفوظ بالجهاز.

والكثير ....

ثالثاً:

هام:

بالنسبة للملفات الخاصة مثل صور العائلة والفيديو احذر من وجودها على كمبيوتر موصول على شبكة الانترنت دون اتخاذ الحيطة واذا تستطيع احفظها على اقراص مدمجة او (السيديات)او الميموري كارد

هناك بعض الخطوات ربما تفي بالغرض لحماية الملفات الخاصة:

ملاحظة: (هذه الخطوات لا تستعصي على الهاكر فأحذر)

-يوجد برامج لحفظ الملفات بكلمة مرور اي تقوم بتشفير الملفات

تستطيع تحميلها من الانترنت .

-وفي نظام الويندوز سفن win7 يوجد خاصية اساسية في النظام لتشفير محركات الاقراص التي يوجد عليها بياناتك بكلمة مرور وهي خاصية :bit locker

تجدها بالدخول إلى> لوحة التحكم >تشفير المحركات باستخدام bit locker

ولكنني شخصياً لا اثق بها لان الهاكر يملكون برامج متخصصة فقط في فك التشفير.

(فأحذر من ملفاتك الشخصية والخاصة على كمبيوترك إذا كان موصول على الانترنت)

رابعاً:

حماية البريد الالكتروني :

اكثر ملفات التجسس والهاكر تأتي عن طريق البريد الالكتروني .

ملاحظة: عن طريق فتح الايميلات الغير معروفة ربما يتم اختراق بريدك أو معرفة كلمة السر خاصتك أو اختراق جهازك.

ويوجد خطوة هام جداً لعدم حدوث ذلك :

عندما تقوم بفتح ايميل لأول مرة تراه او غير معروف لك

يبعث لك الهاكر فيه ملف تجسس قد يكون صورة او ملف مضغوط

من نوع zip او rarلا تقم بإظهار المرفقات حيث ينبهك البريد (هل تريد اظهار المرفقات او تنزيل المرفقات) فلا تقم بذلك اذا لم تتعرف على هوية المرسل لان الهاكر سوف يبعث لك ملف من الملفات التي ذكرتها سابقاً لكي تضغط عليها أو تشغلها أو سمحت بإظهار الملفات المرفقة لابل بمجرد السماح بذلك ومشاهدة المرفقات اذا كانت صورة او اي شيء يتم سرقت كلمة مرورك للبريد و أحياناً اختراق جهازك وهنا المصيبة فهذه الملفات أو البرامج الخبيثة ذكية جداً فقد تأتي بهيئة اي ملف وصعب جداً التكهن بها فاحذرمن اظهار الملفات المرفقة في البريد الالكتروني المجهول .

خامساً:

الحماية من الاختراق :

يوجد برامج تدعى :جدار الحماية وأشهرها برنامج Zone Alarmووظيفة هذا البرنامج هو معرفة كل العمليات التي تقوم بها على الانترنت ومعرفة البرامج التي تعمل في الخفاء و السماح

بتشغيلها أم لا فاذ كنت تعمل على الانترنت وتتصفح مواقع مشكوك بها يحاول الهاكر اختراق جهازك فينبهك البرنامج فتظهر خيارات هل تريد السماح بالعملية سماح allow -- رفض block

فأنت إذا لم تتعرف على التطبيق فتضغط رفض block

فالبرنامج يعمل كمدير للاتصالات وتستطيع من خلاله معرفة ما يدخل إلى جهازك.

كما يوجد الكثير من برامج الحماية المعروفة كالكاسبر والافاست والافيرا والنود المنتشرة بشكل كبير ويجب تحديثها باستمرار ليتم الكشف عن احدث البرامج الخبيثة مع مراعاة اصدارها فيوجد منها : ١. الانتي فايروس ولايحمي كثيرا من الانترنت

٢. الانترنت سيكيورتي وهو المطلوب.

ملاحظة هامة : يتم اختراق جهازك عن طريقة البريد الالكتروني كما شرحت سابقاً وأيضا عن طريق المواقع المزيفة التي تعمل فقط لسرقة الملفات وتهكير الاجهزة وأيضا عن طريق تحميل بعض الملفات التي يزعم أنها برامج مفيدة كبرامج تشغيل الصوت أو الحماية...... وهي في الحقيقة مزيفة ينتظر النقر أو تشغيله ليتم اختراق جهازك.

وكذلك عن طريق الملفات المضغوطة ببرنامج win rar وهي الاكثر انتشاراً على الانترنت .

خلاصة : وضعت بعض المواضيع في النهاية لوجود مواضيع هامة يجب التركيز عليه و يجهلها الكثيرون .

لا تنسونا من صالح دعائكم

اخوكم عزت

ezat222@hotmail.com